Information in the US-CERT Cyber Security Bulletin is a compilation and includes information published by outside sources, so the information should not be considered the result of US-CERT analysis. Software vulnerabilities are categorized in the appropriate section reflecting the operating system on which the vulnerability was reported; however, this does not mean that the vulnerability only affects the operating system reported since this information is obtained from open-source information.

This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to vulnerabilities that appeared in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

Vulnerabilities

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

Note: Even though a vulnerability may allow several malicious acts to be performed, only the highest level risk will be defined in the Risk column.

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
ALWIL Software Avast! Antivirus Home Edition 4.6, Professional Edition 4.6	A vulnerability has been reported in the Aavmker4 device driver due to an insecure memory copy operation, which could let a malicious user obtain elevated privileges. Updates available at: http://www.avast.com/eng/updates.html Currently we are not aware of any exploits for this vulnerability.	ALWIL Software Avast! Antivirus Aavmker4 Device Driver Elevated Privileges CAN-2005-1770	Medium	Bugtraq, 399039, May 26, 2005
Bungie Studios Halo: Combat Evolved 1.06 and 1.00 (Custom Edition) and prior	A vulnerability has been reported that could let remote malicious users cause a Denial of Service. The vulnerability is caused due to an error in the communication handling. The vulnerability will reportedly be fixed in version 1.07. A Proof of Concept exploit has been published.	Halo: Combat Evolved Denial of Service Vulnerability CAN-2005-1741	Low	Luigi Auriemma, May 24, 2005 Secunia SA15501, May 24, 2005

Clever's Games Terminator 3: War of the Machines 1.16	Several vulnerabilities have been reported: a buffer overflow vulnerability was reported due to insufficient boundary checks before copying user-supplied data in sensitive process buffers, which could let a remote malicious user execute arbitrary code; and a remote Denial of Service vulnerability was reported due to a failure to handle exceptional conditions. No workaround or patch available at time of publishing. An exploit script has been published for the buffer overflow vulnerability.	Clever's Games Terminator 3: War of the Machines Remote Buffer Overflow & Denial of Service CAN-2005-1772 CAN-2005-1775	High	Security Focus, 13776 & 13779, May 26, 2005
Computer Associates CA InoculateIT 6.0; eTrust Antivirus r6.0, r7.0, r7.1, eTrust Antivirus for the Gateway r7.0, r7.1, eTrust Secure Content Manager, eTrust Intrusion Detection; BrightStor ARCserve Backup (BAB) r11.1 Windows; eTrust EZ Antivirus r6.2 - r7.0.5, eTrust EZ Armor r1.0 - r2.4.4, eTrust EZ Armor LE r2.0 - r3.0.0.14; Vet Antivirus r10.66 & prior	A vulnerability has been reported in Computer Associates Vet Antivirus engine that could let a remote user execute arbitrary code. A remote user can create a specially crafted Microsoft Office document that will trigger an integer overflow and execute arbitrary code. A fix is available for most of the affected products: http://www3.ca.com/securityadvisor/vulninfo/vuln.aspx?id=32896 The fix is available automatically as part of the daily Vet Signature updates (May 3, 2005). Currently we are not aware of any exploits for this vulnerability.	Computer Associates eTrust Antivirus Integer Overflow in Processing Microsoft OLE Data Lets Remote Users Execute Arbitrary Code CAN-2005-1693	High	Computer Associates, Vulnerability ID: 32896, May 25, 2005
Compuware DriverStudio 3.1, 3.2	A remote Denial of Service vulnerability has been reported due to an error in the 'DbgMsg.sys' driver. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Compuware Softice 'DbgMsg.sys' Remote Denial of Service	Low	Securiteam, May 31, 2005
dotnetindex Active News Manager 2.x	A vulnerability has been reported that could let remote malicious users conduct SQL injection attacks. Input passed to the username and password fields in 'login.asp' isn't properly validated. No workaround or patch available at time of publishing. There is no exploit script required; however, a Proof of Concept exploit has been published.	Active News Manager Username and Password SQL Injection CAN-2005-1780	High	Secunia SA15493, May 25, 3005
Firefly Studios Stronghold 2 1.2	A remote Denial of Service vulnerability has been reported due to an error when handling overly long nicknames. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Firefly Studios Stronghold 2 Remote Denial of Service CAN-2005-1808	Low	Securiteam, May 31, 2005
FutureSoft TFTP Server 2000 1.0 .0.1	Several vulnerabilities were reported: a buffer overflow vulnerability was reported due to boundary errors when handling Read and Write requests, which could let a remote malicious user execute arbitrary code; and a Directory Traversal vulnerability was reported due to insufficient input validation, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	FutureSoft TFTP Server 2000 Directory Traversal & Buffer Overflows	High	SIG^2 Vulnerability Research Advisory, May 31, 2005
Hosting Controller Hosting Controller 6.1, Hotfixes 2.0, 1.9, 1.7, 1.4	A vulnerability has been reported in 'UserProfile.asp' due to insufficient authentication, which could let a malicious user bypass authentication and modify profile information. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	Hosting Controller 'UserProfile.asp' Authentication Bypass CAN-2005-1784	Medium	Security Tracker Alert, 1014062, May 27, 2005
Hosting Controller Hosting Controller 6.x	An SQL injection vulnerability has been reported in 'resellerresources.asp' due to insufficient sanitization of the 'jresourceid' parameter before used in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Hosting Controller 'resellerresources.asp' SQL Injection CAN-2005-1788	High	Secunia Advisory, SA15540, May 30, 2005
India Software Solution Shopping Cart	An SQL injection vulnerability has been reported in the 'shopcart/signin.asp' script due to insufficient validation of the 'password' parameter, which could let a remote malicious user execute arbitrary SQL commands. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	India Software Solution Shopping Cart 'signin.asp' SQL Injection CAN-2005-1789	High	Security Tracker Alert, 1014074, May 29, 2005

MailEnable MailEnable Enterprise Edition 1.x, MailEnable Professional 1.x	A vulnerability has been reported during SMTP authentication, which could let a remote malicious user cause a Denial of Service. Apply update: http://www.mailenable.com/hotfix/MEIMSM-HF050523.zip Currently we are not aware of any exploits for this vulnerability.	MailEnable Unspecified SMTP Authentication Denial of Service CAN-2005-1781	Low	Secunia SA15487, May 26, 3006
MaxWebPortal.com MaxWebPortal 1.35, 1.36, 2.0, 20050418 Next	An input validation vulnerability has been reported in the 'password.asp' script that could let a remote user inject SQL commands. The 'memKey' parameter is not properly validated. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	MaxWebPortal Input Validation Hole in 'password.asp' Permits SQL Injection CAN-2005-1779	High	Security Tracker Alert, 014048, May 25, 2005
Microsoft Internet Explorer 6.0 SP2	A remote Denial of Service vulnerability has been reported when the browser handles a specially crafted JavaScript 'onLoad' handler. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Microsoft Internet Explorer JavaScript OnLoad Handler Remote Denial of Service CAN-2005-1790	Low	Secunia Advisory, SA15546, May 31, 2005
Microsoft Internet Explorer 6.0 SP2	A remote Denial of Service vulnerability has been reported when a malformed URI is added to the list of restricted sites. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Microsoft Internet Explorer Restricted Sites Malformed URI Remote Denial of Service CAN-2005-1791	Low	Security Focus, 13798, May 31, 2005
Microsoft RDP 4.0, 5.0-5.2	A vulnerability has been reported because a private key that is used to sign the Terminal Server public key is hardcoded in a DLL, which could let a remote malicious user conduct man-in-the-middle attacks. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Microsoft Windows Remote Desktop Protocol Server Private Key Disclosure CAN-2005-1794	Medium	Security Focus, 13818, May 31, 2005
Microsoft Windows 98SE	A remote Denial of Service vulnerability has been reported in the 'user32.dll' library when icon files that contain large size values are submitted. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Microsoft Windows 'User32.DLL' Icon Handling Remote Denial of Service CAN-2005-1793	Low	Bugtraq, 399207, May 25, 2005
Microsoft Windows XP Home, SP1 & SP2, XP Professional, SP1 & SP2	A Denial of Service vulnerability has been reported when a malicious user generates excessive expired and unused security contexts. Microsoft has released KB article 890196 to address this issue available at: http://support.microsoft.com/kb/890196/EN-US/#appliesto Currently we are not aware of any exploits for this vulnerability.	Microsoft Windows XP Windows Management Instrumentation Denial of Service CAN-2005-1792	Low	Networksecurity.fi Security Advisory, May 28, 2005
Microsoft Windows Media Player 9 Series, Windows Messenger 5.0, MSN Messenger 6.1, 6.2	Several vulnerabilities exist: a vulnerability exists in Media Player due to a failure to properly handle PNG files that contain excessive width or height values, which could let a remote malicious user execute arbitrary code; and a vulnerability exists in the Windows and MSN Messenger due to a failure to properly handle corrupt or malformed PNG files, which could let a remote malicious user execute arbitrary code. Patches available at: http://www.microsoft.com/technet/security/bulletin/MS05-009.mspx V1.1: Bulletin updated with information on the mandatory upgrade of vulnerable MSN Messenger clients in the caveat section, as well as changes to the Workarounds for PNG Processing Vulnerability in MSN Messenger. V1.2: Bulletin updated with correct file version information for Windows Messenger 5.0 update, as well as added Windows Messenger 5.1 to "Non-Affected Software" list. V2.0: The update for Windows Messenger version 4.7.0.2009 (when running on Windows XP Service Pack 1) was failing to install when distributed via SMS or AutoUpdate. An updated package	Microsoft Media Player & Windows/MSN Messenger PNG Processing CAN-2004-1244 CAN-2004-0597	High	Microsoft Security Bulletin, MS05-009, February 8, 2005 US-CERT Technical Cyber Security Alert TA05-039A US-CERT Cyber Security Alert SA05-039A US-CERT Vulnerability Note VU#259890 Security Focus, February 10, 2005 Microsoft Security Bulletin MS05-009 V1.1, February 11, 2005 Microsoft Security

	corrects this behavior. V2.1: Bulletin updated to update the "Security Update Information" section for the Microsoft Windows Messenger 4.7.0.2009 (when running on Windows XP Service Pack 1) security update. V2.2: Updated the "deployment" section of Microsoft Windows Messenger version 4.7.0.2009 for the correct command. **V2.3: Updated the "Security Update Information" section for Microsoft Windows Messenger version 4.7.0.2009 with the correct setup switches.** An exploit script has been published for MSN Messenger/Windows Messenger PNG Buffer Overflow vulnerability.			Bulletin, MS05-009 V1.2, February 15, 2005 Microsoft Security Bulletin, MS05-009 V2.0, April 12, 2005 Microsoft Security Bulletin, MS05-009 V2.1, May 11, 2005 Microsoft Security Bulletin, MS05-009 V2.2, May 11, 2005 **Microsoft Security Bulletin, MS05-009 V2.3, May 25, 2005**
Newmad Technologies PicoWebServer 1.0	A buffer overflow vulnerability has been reported when handling long HTTP GET requests, which could let a remote malicious user cause a Denial or Service or execute arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Newmad Technologies PicoWebServer Remote Buffer Overflow	High	Security Focus, 13807, May 28, 2005
os4e	An SQL injection vulnerability has been reported in the 'login.asp' script due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	OS4E 'LOGIN.ASP' SQL Injection CAN-2005-1805	High	Security Focus, 13804, May 28, 2005
ServersCheck ServersCheck 5.9 .0, 5.10 .0	A Directory Traversal vulnerability has been reported due to insufficient validation of user-supplied input, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	ServersCheck Directory Traversal CAN-2005-1798	Medium	Security Tracker Alert, 1014075, May 29, 2005
WMR Simpson BookReview 1.0 beta	Several vulnerabilities have been reported: an input validation vulnerability was reported that could let a remote malicious user conduct Cross-Site Scripting attacks. Several scripts are affected: 'index.php,' 'add_contents.htm,' 'add_review.htm,' 'suggest_category.htm,' 'contact.htm,' 'add_booklist.htm,' 'add_url.htm,' 'search.htm,' 'suggest_review.htm,' and 'add_classification.htm;' and a vulnerability was reported because remote malicious user can obtain the path of the web server via certain parameters to search.htm. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	BookReview Input Validation Holes Permit Cross-Site Scripting & Path Disclosure CAN-2005-1782 CAN-2005-1783	High	Security Tracker Alert, 1014058, May 26 2005
zon.cn ZonGG 1.2	A vulnerability has been reported that could let a remote malicious user inject SQL commands. The 'ad/login.asp' script does not properly validate user-supplied input in the password parameter. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	ZonGG Input Validation Hole in 'ad/login.asp' Permits SQL Injection CAN-2005-1785	High	Security Tracker Alert, 1014063, May 27, 2005

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
4D Inc. WebSTAR 5.3.3, 5.4	A buffer overflow vulnerability has been reported in the Tomcat plugin due to a boundary error when processing URLs, which could let a remote malicious user cause a Denial of Service and potentially execute arbitrary code. **Updates available at:** **http://www.4d.com/products/downloads_4dws.html** An exploit script has been published.	4D WebStar Tomcat Plugin Remote Buffer Overflow CAN-2005-1507	High	Securiteam, May 8, 2005 **Security Focus, 13538, May 26, 2005**

Apple Keynote 2, 2.0.1	A vulnerability has been reported that could let a remote malicious user obtain files from the target user's system. A remote user can create a specially crafted Keynote presentation that, when loaded by the target user via the 'keynote:' URL handler, can access files on the target user's system. A fixed version (2.0.2) is available via Software Updates or at: http://www.apple.com/support/downloads/ Currently we are not aware of any exploits for this vulnerability.	Apple Keynote 'keynote:' Lets Remote Users Access Local Files CAN-2005-1408	Medium	Apple Security Advisory, Article ID: 301713, May 25, 2005
bzip2 bzip2 1.0.2 & prior	A vulnerability has been reported when an archive is extracted into a world or group writeable directory, which could let a malicious user modify file permissions of target files. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/b/bzip2/ Mandriva: http://www.mandriva.com/security/advisories **Debian:** **http://security.debian.org/pool/updates/main/b/bzip2/** There is no exploit code required.	BZip2 File Permission Modification CAN-2005-0953	Medium	Security Focus, 12954, March 31, 2005 Ubuntu Security Notice, USN-127-1, May 17, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:091, May 19, 2005 **Debian Security Advisory, DSA 730-1, May 27, 2005**
Clam Anti-Virus ClamAV 0.80 rc4, 0.81-0.83, 0.84 rc1 & rc2	A vulnerability has been reported in 'shared/misc.c' in the 'filecopy()' function when an affected file cannot be removed, which could let a malicious user execute arbitrary code. Upgrades avail bale at: http://prdownloads.sourceforge.net/clamav/clamav-0.85.1.tar.gz?download There is no exploit code required.	Clam Anti-Virus ClamAV Mac OS X Command Execution CAN-2005-1795	High	Security Tracker Alert, 1014070, May 28, 2005
Ethereal Group Ethereal 0.8.14, 0.8.15, 0.8.18, 0.8.19, 0.9-0.9.16, 0.10-0.10.9	Multiple vulnerabilities were reported that affects more 50 different dissectors, which could let a remote malicious user cause a Denial of Service, enter an endless loop, or execute arbitrary code. The following dissectors are affected: 802.3 Slow, AIM, ANSI A, BER, Bittorrent, CMIP, CMP, CMS, CRMF, DHCP, DICOM, DISTCC, DLSw, E IGRP, ESS, FCELS, Fibre Channel, GSM, GSM MAP, H.245, IAX2, ICEP, ISIS, ISUP, KINK, L2TP, LDAP, LMP, MEGACO, MGCP, MRDISC, NCP, NDPS, NTLMSSP, OCSP, PKIX Qualified, PKIX1Explitit, Presentation, Q.931, RADIUS, RPC, RSVP, SIP, SMB, SMB Mailslot, SMB NETLOGON, SMB PIPE, SRVLOC, TCAP, Telnet, TZSP, WSP, and X.509. Upgrades available at: http://www.ethereal.com/distribution/ethereal-0.10.11.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200505-03.xml Mandriva: http://www.mandriva.com/security/advisories **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-427.html** **An exploit script has been published.**	Ethereal Multiple Remote Protocol Dissector Vulnerabilities CAN-2005-1456 CAN-2005-1457 CAN-2005-1458 CAN-2005-1459 CAN-2005-1460 CAN-2005-1461 CAN-2005-1462 CAN-2005-1463 CAN-2005-1464 CAN-2005-1465 CAN-2005-1466 CAN-2005-1467 CAN-2005-1468 CAN-2005-1469 CAN-2005-1470	High	Ethereal Security Advisory, enpa-sa-00019, May 4, 2005 Gentoo Linux Security Advisory, GLSA 200505-03, May 6, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:083, May 11, 2005 **RedHat Security Advisory, RHSA-2005:427-05, May 24, 2005**
Ettercap Ettercap 0.6 .b, 0.6 .a, 0.6.3.1, 0.6.4, 0.6.5, 0.6.6 .6, 0.6.7, 0.6.9, Ettercap-NG 0.7 .0-0.7.2	A format string vulnerability has been reported in the 'curses_msg()' function in the Ncurses interface, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://prdownloads.sourceforge.net/ettercap/ettercap-NG-0.7.3.tar.gz?download Currently we are not aware of any exploits for this vulnerability.	Ettercap Remote Format String CAN-2005-1796	High	Secunia Advisory, SA15535, May 31, 2005
GNU Mailutils 0.5, 0.6	Multiple vulnerabilities have been reported that could let a remote malicious user execute arbitrary code or cause a Denial of Service. These vulnerabilities are due to a buffer overflow in the 'header_get_field_name()' function in 'mailbox/header.c'; an integer overflow in the 'fetch_io()' function; an input validation error in the imap4d server in the FETCH command; and a format string flaw in the imap4d server. A fixed version (0.6.90) is available at: ftp://alpha.gnu.org/gnu/mailutils/mailutils-0.6.90.tar.gz Gentoo:	GNU Mailutils Buffer Overflow and Format String Bugs Let Remote Users Execute Arbitrary Code CAN-2005-1520 CAN-2005-1521 CAN-2005-1522 CAN-2005-1523	High	iDEFENSE Security Advisory 05.25.05 Gentoo Linux Security Advisory, GLSA 200505-20, May 27, 2005

	http://security.gentoo.org/ glsa/glsa-200505-20.xml Proofs of Concept exploits have been published.			
GNU shtool 2.0.1 & prior	A vulnerability has been reported that could let a local malicious user gain escalated privileges. The vulnerability is caused due to temporary files being created insecurely. No workaround or patch available at time of publishing. There is no exploit code required.	GNU shtool Insecure Temporary File Creation CAN-2005-1751	Medium	Secunia Advisory, SA15496, May 25, 2005
Hewlett Packard Company HP-UX B.11.23, B.11.22, B.11.11, B.11.04, B.11.00	A remote Denial of Service vulnerability has been reported in the Path MTU Discovery (PMTUD) functionality that is supported in the ICMP protocol. Patches available at: http://www1.itrc.hp.com/service/ cki/docDisplay.do?docId= HPSBUX01137 Currently we are not aware of any exploits for this vulnerability.	HP-UX ICMP PMTUD Remote Denial of Service CAN-2005-1192	Low	Hewlett Packard Company Security Advisory, HPSBUX01137, April 24, 2005 **Hewlett Packard Company Security Advisory, HPSBUX01137: SSRT5954 rev.1, May 25, 2005**
Hewlett-Packard HP-UX B.11.00, B.11.11, B.11.22, B.11.23; only if converted to trusted systems	A vulnerability has been reported that could let a remote malicious user access the system. HP-UX systems that have been converted to trusted systems contain an unspecified vulnerability that allows a remote user to gain unauthorized access to the target system. The vendor has issued the following fixes, available at: http://itrc.hp.com For HP-UX B.11.00 - PHCO_29249 and PHNE_17030 For HP-UX B.11.11 - PHCO_33215 For HP-UX B.11.23 - PHCO_32926 For HP-UX B.11.22, action: disable remshd (OS-Core.CORE2-SHLIBS) and avoid the telnet -t option. Currently we are not aware of any exploits for this vulnerability.	HP-UX Trusted Systems Grant Access to Remote Users CAN-2005-1771	Medium	HP Security Bulletin, HPSBUX01165 REVISION: 0, SSRT5899 rev.0, May 25, 2005
Multiple Vendors ImageMagick 6.0-6.0.8, 6.1-6.1.8, 6.2 .0.7, 6.2 .0.4, 6.2, 6.2.1	A buffer overflow vulnerability has been reported due to a failure to properly validate user-supplied string lengths before copying into static process buffers, which could let a remote malicious user cause a Denial of Service. Upgrades available at: http://www.imagemagick.org/ script/binary-releases.php Fedora: http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/3/ Ubuntu: http://security.ubuntu.com/ ubuntu/pool/main/i/imagemagick/ **RedHat:** **http://rhn.redhat.com/ errata/RHSA-2005-413.html** A Proof of Concept exploit has been published.	ImageMagick Remote Buffer Overflow CAN-2005-1275	Low	Security Focus, 13351, April 25, 2005 Fedora Update Notification FEDORA-2005-344, April 28, 2005 Ubuntu Security Notice, USN-132-1 May 23, 2005, May 23, 2005 **RedHat Security Advisory, RHSA-2005:413-04, May 25, 2005**
Multiple Vendors KDE 2.0, beta, 2.0.1, 2.1-2.1.2, 2.2-2.2.2, 3.0-3.0.5, 3.1-3.1.5, 3.2-3.2.3, 3.3-3.3.2, 3.4; Novell Linux Desktop 9; SuSE Linux 9.1, x86_64, 9.2, x86_64, 9.3, Linux Enterprise Server 9	A buffer overflow vulnerability has been reported in the 'kimgio' image library due to insufficient validation of PCX image data, which could let a remote malicious user cause a Denial of Service or possibly execute arbitrary code. Patches available at: http://bugs.kde.org/attachment.cgi ?id=10325&action=view http://bugs.kde.org/attachment.cgi ?id=10326&action=view SuSE: ftp://ftp.suse.com/pub/suse/ Gentoo: http://security.gentoo.org/ glsa/glsa-200504-22.xml Debian: http://security.debian.org/ pool/updates/main/k/kdelibs/ Fedora: http://download.fedora.redhat.com/	KDE 'kimgio' image library Remote Buffer Overflow CAN-2005-1046	High	SUSE Security Announcement, SUSE-SA:2005:022, April 11, 2005 Gentoo Linux Security Advisory, GLSA 200504-22, April 22, 2005 Debian Security Advisory, DSA 714-1, April 26, 2005 Fedora Update Notification, FEDORA-2005-350, May 2, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:085, May 12, 2005 Conectiva Linux

	pub/fedora/linux/core/updates/3/ Ubuntu: http://security.ubuntu.com/ ubuntu/pool/main/k/kdelibs/ Mandriva: http://www.mandriva.com/ security/advisories Conectiva: ftp://atualizacoes.conectiva.com.br/ RedHat: http://rhn.redhat.com/ errata/RHSA-2005-393.html **Ubuntu: http://security.ubuntu.com/ ubuntu/pool/main/k/kdelibs/** Denial of Service Proofs of Concept exploits have been published.			Security Announcement, CLA-2005:953, May 17, 2005 RedHat Security Advisory, RHSA-2005:393-05, May 17, 2005 SUSE Security Summary Report, SUSE-SR:2005:013, May 18, 2005 **Ubuntu Security Notice, USN-114-2, May 27, 2005**
Multiple Vendors AES AES (Rijndael); OpenSSL Project OpenSSL 0.9.1-0.9.7	A vulnerability has been reported in high-speed implementations of AES due to the time taken to complete certain critical AES cryptographic functions (Input dependant Table lookups), which could let a remote malicious user retrieve an entire AES secret key from a target vulnerable AES implementation. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Multiple Vendor Advanced Encryption Standard Cache Timing Key Disclosure CAN-2005-1797	Medium	Security Focus, 13785, May 26, 2005
Multiple Vendors Gentoo Linux; GNU GDB 6.3	Multiple vulnerabilities have been reported: a heap overflow vulnerability was reported when loading malformed object files, which could let a remote malicious user execute arbitrary code; and a vulnerability was reported which could let a malicious user obtain elevated privileges. Gentoo: http://security.gentoo.org/ glsa/glsa-200505-15.xml **Ubuntu: http://security.ubuntu.com/ ubuntu/pool/main/g/gdb/** **http://security.ubuntu.com/ ubuntu/pool/main/b/binutils/** **Mandriva: http://www.mandriva.com/ security/advisories** **Trustix: http://http.trustix.org/ pub/trustix/updates/** Currently we are not aware of any exploits for these vulnerabilities.	GDB Multiple Vulnerabilities CAN-2005-1704 CAN-2005-1705	High	Gentoo Linux Security Advisory, GLSA 200505-15, May 20, 200 **Ubuntu Security Notices, USN-135-1, 136-1 & 136-2, May 27, 2005** **Mandriva Linux Security Update Advisory, MDKSA-2005:09, May 30, 2005** **Trustix Secure Linux Security Advisory, TSL-2005-0025, May 31, 2005**
Multiple Vendors GraphicsMagick GraphicsMagick 1.0, 1.0.6, 1.1, 1.1.3-1.1.6; ImageMagick ImageMagick 5.3.3, 5.3.8, 5.4.3, 5.4.4 .5, 5.4.7, 5.4.8, 5.5.3.2-1.2.0, 5.5.4, 5.5.6 .0-20030409, 5.5.6, 5.5.7, 6.0-6.0.8, 6.1-6.1.8, 6.2.0.7, 6.2 .0.4, 6.2-6.2.2	A remote Denial of Service vulnerability has been reported due to a failure to handle malformed XWD image files. Gentoo: http://security.gentoo.org/ glsa/glsa-200505-16.xml **Ubuntu: http://security.ubuntu.com/ ubuntu/pool/main/i/imagemagick/** **Fedora: http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/3/** Currently we are not aware of any exploits for this vulnerability.	ImageMagick & GraphicsMagick XWD Decoder Remote Denial of Service CAN-2005-1739	Low	Gentoo Linux Security Advisory, GLSA 200505-16, May 21, 2005 **Ubuntu Security Notice, USN-132-1, May 23, 2005** **Fedora Update Notification, FEDORA-2005-395, May 26, 2005**
Multiple Vendors Linux kernel 2.2.x, 2.4.x, 2.6.x	A buffer overflow vulnerability has been reported in the 'elf_core_dump()' function due to a signedness error, which could let a malicious user execute arbitrary code with ROOT privileges. Update available at: http://kernel.org/ Trustix: http://www.trustix.org/ errata/2005/0022/ Ubuntu: http://security.ubuntu.com/	Linux Kernel ELF Core Dump Buffer Overflow CAN-2005-1263	High	Secunia Advisory, SA15341, May 12, 2005 Trustix Secure Linux Security Advisory, 2005-0022, May 13, 2005 Ubuntu Security Notice, USN-131-1, May 23, 2005 **RedHat Security**

	ubuntu/pool/main/l/ **RedHat:** **http://rhn.redhat.com/ errata/RHSA-2005-472.html** **An exploit script has been published.**			**Advisory, RHSA-2005:472-05, May 25, 2005**
Multiple Vendors Linux Kernel 2.4.0-test1-test12, 2.4-2.4.30, 2.5.0- 2.5.69, 2.6 -test1-test11, 2.6- 2.6.9	A vulnerability has been reported in both cryptoloop and dm-crypt because certain watermarked files may be disclosed, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. Exploit scripts have been published.	Linux Kernel Cryptoloop Information Disclosure CAN-2004-2135 CAN-2004-2136	Medium	Securiteam, May 26, 2005
Multiple Vendors Linux kernel 2.6.10, 2.6 -test9-CVS, 2.6-test1- -test11, 2.6, 2.6.1-2.6.11 ; RedHat Desktop 4.0, Enterprise Linux WS 4, ES 4, AS 4	Multiple vulnerabilities exist: a vulnerability exists in the 'shmctl' function, which could let a malicious user obtain sensitive information; a Denial of Service vulnerability exists in 'nls_ascii.c' due to the use of incorrect table sizes; a race condition vulnerability exists in the 'setsid()' function; and a vulnerability exists in the OUTS instruction on the AMD64 and Intel EM64T architecture, which could let a malicious user obtain elevated privileges. RedHat: https://rhn.redhat.com/errata/ RHSA-2005-092.html Ubuntu: http://security.ubuntu.com/ubuntu/ pool/main/l/linux-source-2.6.8.1/ Conectiva: ftp://atualizacoes.conectiva. com.br/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Fedora: http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/2/ Conectiva: ftp://atualizacoes.conectiva. com.br/10/ Fedora: http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/ errata/RHSA-2005-366.html RedHat: http://rhn.redhat.com/ errata/RHSA-2005-283.html http://rhn.redhat.com/ errata/RHSA-2005-284.html **RedHat:** **http://rhn.redhat.com/ errata/RHSA-2005-472.html** Currently we are not aware of any exploits for these vulnerabilities.	Linux Kernel Multiple Vulnerabilities CAN-2005-0176 CAN-2005-0177 CAN-2005-0178 CAN-2005-0204	Medium	Ubuntu Security Notice, USN-82-1, February 15, 2005 RedHat Security Advisory, RHSA-2005:092-14, February 18, 2005 SUSE Security Announcement, SUSE-SA:2005:018, March 24, 2005 Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005 Conectiva Linux Security Announcement, CLA-2005:945, March 31, 2005 Fedora Update Notification FEDORA-2005-313, April 11, 2005 RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005 RedHat Security Advisories, RHSA-2005:283-15 & RHSA-2005:284-11, April 28, 2005 **RedHat Security Advisory, RHSA-2005:472-05, May 25, 2005**
Multiple Vendors Qpopper 4.x; Gentoo Linux	Several vulnerabilities have been reported: a vulnerability was reported because user supplied config and trace files are processed with elevated privileges, which could let a malicious user create/overwrite arbitrary files; and a vulnerability was reported due to an unspecified error which could let a malicious user create group or world-writable files. Upgrades available at: ftp://ftp.qualcomm.com/eudora/ servers/unix/popper/old/qpopper4.0.5.tar.gz Gentoo: http://security.gentoo.org/ glsa/glsa-200505-17.xml **Debian:** **http://security.debian.org/ pool/updates/main/q/qpopper/** There is no exploit code required.	Qpopper Multiple Insecure File Handling CAN-2005-1151 CAN-2005-1152	Medium	Gentoo Linux Security Advisory GLSA 200505-17, May 23, 2005 Secunia Advisory, SA15475, May 24, 2005 Debian Security Advisories, DSA 728-1 & 728-2, May 25 & 26, 2005

Multiple Vendors X.org X11R6 6.7.0, 6.8, 6.8.1; XFree86 X11R6 3.3, 3.3.2-3.3.6, 4.0, 4.0.1, 4.0.2 -11, 4.0.3, 4.1.0, 4.1 -12, 4.1 -11, 4.2 .0, 4.2.1 Errata, 4.2.1, 4.3.0.2, 4.3.0.1, 4.3.0	An integer overflow vulnerability exists in 'scan.c' due to insufficient sanity checks on on the 'bitmap_unit' value, which could let a remote malicious user execute arbitrary code. Patch available at: https://bugs.freedesktop.org/attachment.cgi?id=1909 Gentoo: http://security.gentoo.org/glsa/glsa-200503-08.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/lesstif1-1/ Gentoo: http://security.gentoo.org/glsa/glsa-200503-15.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/x/xfree86/ ALTLinux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-331.html SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-044.html Mandrake: http://www.mandrakesecure.net/en/ftp.php Mandriva: http://www.mandriva.com/security/advisories Debian: http://security.debian.org/pool/updates/main/x/xfree86/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-412.html **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-473.html** Currently we are not aware of any exploits for this vulnerability.	LibXPM Bitmap_unit Integer Overflow CAN-2005-0605	High	Security Focus, 12714, March 2, 2005 Gentoo Linux Security Advisory, GLSA 200503-08, March 4, 2005 Ubuntu Security Notice, USN-92-1 March 07, 2005 Gentoo Linux Security Advisory, GLSA 200503-15, March 12, 2005 Ubuntu Security Notice, USN-97-1 March 16, 2005 ALTLinux Security Advisory, March 29, 2005 Fedora Update Notifications, FEDORA-2005-272 & 273, March 29, 2005 RedHat Security Advisory, RHSA-2005: 331-06, March 30, 2005 SGI Security Advisory, 20050401-01-U, April 6, 2005 RedHat Security Advisory, RHSA-2005:044-15, April 6, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:080, April 29, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:081, May 6, 2005 Debian Security Advisory, DSA 723-1, May 9, 2005 RedHat Security Advisory, RHSA-2005:412-05, May 11, 2005 **RedHat Security Advisory, RHSA-2005:473-03, May 24, 2005**
PHP Group PHP 4.3-4.3.10; Peachtree Linux release 1	A remote Denial of Service vulnerability has been reported when processing deeply nested EXIF IFD (Image File Directory) data. Upgrades available at: http://ca.php.net/get/php4.3.11.tar.gz/from/a/mirror Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/php4/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-15.xml Fedora: http://download.fedora.redhat.com/	PHP Group Exif Module IFD Nesting Remote Denial of Service CAN-2005-1043	Low	Security Focus, 13164, April 14, 2005 Ubuntu Security Notice, USN-112-1, April 14, 2005 Gentoo Linux Security Advisory, GLSA 200504-15, April 18, 2005 Fedora Update Notification, FEDORA-2005-315, April 18, 2005

	pub/fedora/linux/core/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Peachtree: http://peachtree.burdell.org/updates/ SGI: ftp://patches.sgi.com/support/free/security/advisories/ **Conectiva:** **http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000955** Currently, we are not aware of any exploits for this vulnerability.			Mandriva Linux Security Update Advisory, MDKSA-2005:072, April 19, 2005 Peachtree Linux Security Notice, PLSN-0001, April 21, 2005 SGI Security Advisory, 20050501-01-U, May 5, 2005 **Conectiva Security Advisory, CLSA-2005:955, May 31, 2005**
PHP Group PHP 4.3-4.3.10; Peachtree Linux release 1	A vulnerability has been reported in the 'exif_process_IFD_TAG()' function when processing malformed IFD (Image File Directory) tags, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://ca.php.net/get/php4.3.11.tar.gz/from/a/mirror Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/php4/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-15.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Peachtree: http://peachtree.burdell.org/updates/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-405.html SUSE: ftp://ftp.SUSE.com/pub/SUSE SGI: ftp://patches.sgi.com/support/free/security/advisories/ **Conectiva:** **http://distro.conectiva.com.br/atualizacoes/index.php?id=a&anuncio=000955** Currently, we are not aware of any exploits for this vulnerability.	PHP Group Exif Module IFD Tag Integer Overflow CAN-2005-1042	High	Security Focus, 13163, April 14, 2005 Ubuntu Security Notice, USN-112-1, April 14, 2005 Gentoo Linux Security Advisory, GLSA 200504-15, April 18, 2005 Fedora Update Notification, FEDORA-2005-315, April 18, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:072, April 19, 2005 Peachtree Linux Security Notice, PLSN-0001, April 21, 2005 Turbolinux Security Advisory, TLSA-2005-50, April 28, 2005 RedHat Security Advisory, RHSA-2005:405-06, April 28, 2005 SUSE Security Summary Report, SUSE-SR:2005:012, April 29, 2005 SGI Security Advisory, 20050501-01-U, May 5, 2005 **Conectiva Security Advisory, CLSA-2005:955, May 31, 2005**
SCO Open Server 5.0.7	A buffer overflow vulnerability has been reported in 'nwprint' due to insufficient bounds checking, which could let a malicious user obtain elevated privileges. **SCO:** **ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2005.26** An exploit script has been published.	SCO OpenServer NWPrint Command Buffer Overflow **CAN-2005-0993**	Medium	Bugtraq, 394864, April 4, 2005 **SCO Security Advisory, SCOSA-2005.26, May 25, 2005**

WEB-DAV Linux File System (davfs2) 0.x	A vulnerability has been reported that could let malicious, local users bypass certain security restrictions. A mounted file system fails to support UNIX permissions. No workaround or patch available at time of publishing. There is no exploit code required.	WEB-DAV Linux File System No Enforcing of UNIX Permissions CAN-2005-1774	Medium	Secunia Advisory, SA15497, May 26, 2005
xine gxine 0.4.0-0.4.4	A format string vulnerability has been reported due to insecure implementation of a formatted printing function, which could let a remote malicious user execute arbitrary code. **Gentoo:** **http://security.gentoo.org/glsa/glsa-200505-19.xml** Currently we are not aware of any exploits for this vulnerability.	GXINE Remote Hostname Format String CAN-2005-1692	High	pst.advisory, May 21, 2005 **Gentoo Linux Security Advisory, GLSA 200505-19, May 26, 2005**

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
C'Nedra C'Nedra 0.4	A buffer overflow vulnerability has been reported in 'game_message_functions.cpp' source file due to a boundary error in 'READ_TCP_STRING()' function, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. An exploit script has been published.	C'Nedra Network Plug-in 'Read_TCP_String' Remote Buffer Overflow CAN-2005-1776	High	Secunia Advisory, SA15519, May 27, 2005
FreeStyle Wiki Wiki 3.5.7, Wiki WikiLite .10	A vulnerability has been reported due to insufficient sanitization of input passed in uploaded attachments, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://prdownloads.sourceforge.jp/fswiki/14800/fswiki_lite_0_0_11.zip There is no exploit code required.	FreeStyle Wiki Attachment HTML Injection CAN-2005-1799	High	Secunia Advisory, SA15538, May 31, 2005
FunkyASP FunkyASPAD System 1.1	A vulnerability has been reported that could let remote malicious users conduct SQL injection attacks. This is due to improper input validation in 'admin.asp.' No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	FunkyASP AD System 'password' SQL Injection Vulnerability CAN-2005-1786	High	Secunia SA15494, May 25, 2005
GPL phpStat	A vulnerability has been reported that could let a remote malicious user gain administrative access to the application. A remote user can supply a specially crafted URL to cause 'setup.php' to reset the password on a username. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit script has been published.	GPL phpStat 'setup.php' Lets Remote Users Modify the Administrative Password CAN-2005-1787	High	SoulBlack Security Research, May 25, 2005
Hummingbird Ltd. Exceed 10.x, 9.x, PowerSuite 10.x, HostExplorer 10.x, Hummingbird Connectivity 9.x, InetD 10.x, NFS Maestro Client 10.x, Gateway 10.x, Server 10.x	Several vulnerabilities have been reported: a buffer overflow vulnerability was reported in the InetD FTPD component (ftpdw.exe) when an overly large argument is passed to a FTP command, which could let a remote malicious user cause a Denial of Service; and a buffer overflow vulnerability was reported due to a boundary error in the he InetD LPD component (Lpdw.exe) when a large amount of data is received, which could let a remote malicious user cause a Denial of Service and possible execute arbitrary code. Patches available at: http://connectivity.hummingbird.com/support/nc Currently we are not aware of any exploits for these vulnerabilities.	Hummingbird InetD Components Buffer Overflow	High	Secunia Advisory, SA15557, May 31, 2005
Invision Power Services Invision Board 1.0, 1.0.1, 1.1.1, 1.1.2, 1.2, 1.3 Final, 1.3, 1.3.1 Final, 2.0 PF1&PF2, 2.0 PDR3, 2.0, Alpha 3, 2.0.1-2.0.4	A vulnerability has been reported due to an error when deleting user groups, which could let a malicious user obtain root administrator privileges. No workaround or patch available at time of publishing.	Invision Power Board Root Privileges	High	Secunia Advisory, SA15545, May 30, 2005

	There is no exploit code required.			
Invision Power Services Invision Board 1.0, 1.0.1, 1.1.1, 1.1.2, 1.2, 1.3 Final, 1.3	A vulnerability was reported because forum posts owned by other moderators can be modified through an HTTP GET request without authentication credentials, which could let a remote malicious user obtain unauthorized access. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Invision Power Board Unauthorized Access	Medium	Security Focus, 13802, May 28, 2005
Invision Power Services Invision Power Board 1.x, 2.x	Several vulnerabilities have been reported: a Cross-Site vulnerability was reported due to insufficient sanitization of the 'highlite' parameter in 'search.php' and 'topics.php,' which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported in 'login.php' due to insufficient sanitization of input passed to a certain cookie ID parameter, which could let a remote malicious user execute arbitrary SQL code. Upgrades available at: http://www.invisionboard.com/ act.ips/download **Another exploit script has been published.**	Invision Power Cross-Site Scripting & SQL Injection	High	GulfTech Security Research Advisory, May 5, 2005 **Security Focus, May 26, 2005**
JAWS JAWS 0.4, 0.5 beta2, 0.5, 0.5.1	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of the 'Glossary' module, which could let a remote malicious user execute arbitrary HTML and script code. The vulnerability has been fixed in the CVS repository. There is no exploit code required; however, a Proof of Concept exploit has been published.	JAWS Glossary Cross-Site Scripting CAN-2005-1800	High	Security Focus, 13795, May 28, 2005
L-Soft LISTSERV 14.3, 1.8d, 1.8e	Multiple vulnerabilities have been reported that could let a remote malicious user cause a Denial or Service or execute arbitrary code. Fixed versions (14.3 level set 2005a and above) are available at: http://www.lsoft.com/download/ listserv.asp http://www.lsoft.com/download/ listservlite.asp Currently we are not aware of any exploits for this vulnerability.	L-Soft LISTSERV Multiple Unspecified Vulnerabilities CAN-2005-1773	High	Security Tracker Alert ID: 1014051, May 25, 2005 NGSSoftware Insight Security Research, May 25, 2005
Mozilla Firefox Preview Release, 0.8, 0.9 rc, 0.9-0.9.3, 0.10, 0.10.1, 1.0-1.0.3	Several vulnerabilities have been reported: a vulnerability was reported due to insufficient protection of 'IFRAME' JavaScript URLS from being executed in the context of another history list URL, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported in 'InstallTrigger .install()' due to insufficient verification of the 'Icon URL' parameter, which could let a remote malicious user execute arbitrary JavaScript code. Workaround: Disable "tools/options/web-Features/>Allow web sites to install software" Slackware: ftp://ftp.slackware.com/ pub/slack ware/ Gentoo: http://security.gentoo.org/ glsa/glsa-200505-11.xml TurboLinux: ftp://ftp.turbolinux.co.jp/ pub/TurboLinux/ TurboLinux/ia32/ RedHat: http://rhn.redhat.com/ errata/RHSA-2005-434.html http://rhn.redhat.com/ errata/RHSA-2005-435.html **Ubuntu:** **http://security.ubuntu.com/ ubuntu/pool/main/m/**	Mozilla Firefox Remote Arbitrary Code Execution CAN-2005-1476 CAN-2005-1477	High	Secunia Advisory, SA15292, May 9, 2005 US-CERT VU#534710 US-CERT VU#648758 Slackware Security Advisory, SSA:2005-135-01, May 15, 2005 Gentoo Linux Security Advisory, GLSA 200505-11, May 16, 2005 Turbolinux Security Advisory, TLSA-2005 -56, May 16, 2005 RedHat Security Advisories, RHSA-2005:434-10 & RHSA-2005:435-10, May 23 & 24, 2005 **Ubuntu Security Notice, USN-134-1, May 26, 2005**

	mozilla-firefox/ Proofs of Concept exploit scripts have been published.			
Mozilla Mozilla Browser prior to 1.7.8; Mozilla Suite prior to 1.7.8; Firefox prior to 1.0.4; Firebird 0.5, 0.6.1, 0.7	A vulnerability was reported due to a failure in the application to properly verify Document Object Model (DOM) property values, which could let a remote malicious user execute arbitrary code. Firefox: http://www.mozilla.org/ products/firefox/ Mozilla Browser Suite: http://www.mozilla.org/ products/mozilla1.x/ TurboLinux:: ftp://ftp.turbolinux.co.jp/pub/ TurboLinux/TurboLinux/ia32/ RedHat: http://rhn.redhat.com/ errata/RHSA-2005-434.html http://rhn.redhat.com/ errata/RHSA-2005-435.html **Ubuntu:** **http://security.ubuntu.com/ ubuntu/pool/main/m/ mozilla-firefox/** Currently we are not aware of any exploits for this vulnerability.	Mozilla Suite And Firefox DOM Property Overrides CAN-2005-1532	High	Mozilla Foundation Security Advisory, 2005-44, May 12, 2005 Turbolinux Security Advisory, TLSA-2005 -56, May 16, 2005 RedHat Security Advisories, RHSA-2005:434-10 & RHSA-2005:435-10, May 23 & 24, 2005 **Ubuntu Security Notice, USN-134-1, May 26, 2005**
Mozilla Mozilla Browser prior to 1.7.8; Mozilla Suite prior to 1.7.8; Firefox prior to 1.0.4; Firebird 0.5, 0.6.1, 0.7	A vulnerability was reported when processing 'javascript:' URLs, which could let a remote malicious user execute arbitrary code. Firefox: http://www.mozilla.org/ products/firefox/ Mozilla Browser Suite: http://www.mozilla.org/ products/mozilla1.x/ TurboLinux:: ftp://ftp.turbolinux.co.jp/pub/ TurboLinux/TurboLinux/ia32/ RedHat: http://rhn.redhat.com/ errata/RHSA-2005-434.html http://rhn.redhat.com/ errata/RHSA-2005-435.html **Ubuntu:** **http://security.ubuntu.com/ ubuntu/pool/main/m/ mozilla-firefox/** Currently we are not aware of any exploits for this vulnerability.	Mozilla Suite And Firefox Wrapped 'javascript:' URLs CAN-2005-1531	High	Mozilla Foundation Security Advisory, 2005-43, May 12, 2005 Turbolinux Security Advisory, TLSA-2005-56, May 16, 2005 RedHat Security Advisories, RHSA-2005:434-10 & RHSA-2005:435-10, May 23 & 24, 2005 **Ubuntu Security Notice, USN-134-1, May 26, 2005**

Multiple Vendors ALT Linux Compact 2.3, Junior 2.3; Apple Mac OS X 10.0-10.0.4, 10.1-10.1.5, 10.2-10.2.8, 10.3-10.3.8, Mac OS X Server 10.0, 10.1-10.1.5, 10.2-10.2.8, 10.3-10.3.8; MIT Kerberos 5 1.0, 5 1.0.6, 5 1.0.8, 51.1-5 1.4; Netkit Linux Netkit 0.9-0.12, 0.14-0.17, 0.17.17; Openwall GNU/*/Linux (Owl)-current, 1.0, 1.1; FreeBSD 4.10-PRERELEASE, 2.0, 4.0 .x, -RELENG, alpha, 4.0, 4.1, 4.1.1 -STABLE, -RELEASE, 4.1.1, 4.2, -STABLEpre122300, -STABLEpre050201, 4.2 -STABLE, -RELEASE, 4.2, 4.3 -STABLE, -RELENG, 4.3 -RELEASE-p38, 4.3 -RELEASE, 4.3, 4.4 -STABLE, -RELENG, -RELEASE-p42, 4.4, 4.5 -STABLEpre2002-03-07, 4.5 -STABLE, -RELENG, 4.5 -RELEASE-p32, 4.5 -RELEASE, 4.5, 4.6 -STABLE, -RELENG, 4.6 -RELEASE-p20, 4.6 -RELEASE, 4.6, 4.6.2, 4.7 -STABLE, 4.7 -RELENG, 4.7 -RELEASE-p17, 4.7 -RELEASE, 4.7, 4.8 -RELENG, 4.8 -RELEASE-p7, 4.8 -PRERELEASE, 4.8, 4.9 -RELENG, 4.9 -PRERELEASE, 4.9, 4.10 -RELENG, 4.10 -RELEASE, 4.10, 4.11 -STABLE, 5.0 -RELENG, 5.0, 5.1 -RELENG, 5.1 -RELEASE-p5, 5.1 -RELEASE, 5.1, 5.2 -RELENG, 5.2 -RELEASE, 5.2, 5.2.1 -RELEASE, 5.3 -STABLE, 5.3 -RELEASE, 5.3, 5.4 -PRERELEASE; SuSE Linux 7.0, sparc, ppc, i386, alpha, 7.1, x86, sparc, ppc, alpha, 7.2, i386 **SGI IRIX 6.5.24-6.5.27**	Two buffer overflow vulnerabilities have been reported in Telnet: a buffer overflow vulnerability has been reported in the 'slc_add_reply()' function when a large number of specially crafted LINEMODE Set Local Character (SLC) commands is submitted, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability has been reported in the 'env_opt_add()' function, which could let a remote malicious user execute arbitrary code. ALTLinux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html Apple: http://wsidecar.apple.com/cgi-bin/nph-reg3rdpty1.pl/product=05529&platform=osx&method=sa/SecUpd2005-003Pan.dmg Debian: http://security.debian.org/pool/updates/main/n/netkit-telnet/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:01/ MIT Kerberos: http://web.mit.edu/kerberos/|advisories/2005-001-patch_1.4.txt Netkit: ftp://ftp.uk.linux.org/pub/linux/Networking/netkit/ Openwall: http://www.openwall.com/Owl/CHANGES-current.shtml RedHat: http://rhn.redhat.com/errata/RHSA-2005-327.html Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57755-1 SUSE: ftp://ftp.SUSE.com/pub/SUSE Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/n/netkit-telnet/ OpenBSD: http://www.openbsd.org/errata.html#telnet Mandrake: http://www.mandrakesecure.net/en/ftp.php Gentoo: http://security.gentoo.org/glsa/glsa-200503-36.xml http://security.gentoo.org/glsa/glsa-200504-01.xml Debian: http://security.debian.org/pool/updates/main/k/krb5/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-04.xml	Telnet Client 'slc_add_reply()' & 'env_opt_add()' Buffer Overflows CAN-2005-0468 CAN-2005-0469	High	iDEFENSE Security Advisory, March 28, 2005 US-CERT VU#291924 Mandrakelinux Security Update Advisory, MDKSA-2005:061, March 30, 2005 Gentoo Linux Security Advisories, GLSA 200503-36 & GLSA 200504-01, March 31 & April 1, 2005 Debian Security Advisory, DSA 703-1, April 1, 2005 US-CERT VU#341908 Gentoo Linux Security Advisory, GLSA 200504-04, April 6, 2005 SGI Security Advisory, 20050401-01-U, April 6, 2005 Sun(sm) Alert Notification, 57761, April 7, 2005 SCO Security Advisory, SCOSA-2005.21, April 8, 2005 Avaya Security Advisory, ASA-2005-088, April 27, 2005 Gentoo Linux Security Advisory, GLSA 200504-28, April 28, 2005 Turbolinux Security Advisory, TLSA-2005-52, April 28, 2005 Sun(sm) Alert Notification, 57761, April 29, 2005 SCO Security Advisory, SCOSA-2005.23, May 17, 2005 **SGI Security Advisory, 20050405-01-P, May 26, 2005**

	SGI: ftp://oss.sgi.com/projects/ sgi_propack/download /3/updates/ SCO: ftp://ftp.sco.com/pub/updates/ UnixWare/SCOSA-2005.21 Sun: http://sunsolve.sun.com/ search/document.do? assetkey=1-26-57761-1 Openwall: http://www.openwall.com/ Owl/CHANGES-current.shtml Avaya: http://support.avaya.com/ elmodocs2/security/ ASA-2005-088_RHSA-2005-330.pdf Gentoo: http://security.gentoo.org/ glsa/glsa-200504-28.xml TurboLinux: ftp://ftp.turbolinux.co.jp/pub/ TurboLinux/TurboLinux/ia32/ Sun: http://sunsolve.sun.com/search/ document.do?assetkey=1-26-57761-1 OpenWall: http://www.openwall.com/ Owl/CHANGES-current.shtml SCO: ftp://ftp.sco.com/pub/updates/ OpenServer/SCOSA-2005.23 **SGI IRIX:** **Apply patch 5892 for IRIX 6.5.24-6.5.27:** **ftp://patches.sgi.com/ support/free/security/patches/** Currently we are not aware of any exploits for these vulnerabilities.			
Multiple Vendors Cisco Systems Cisco Aironet 1200 Series Access Point, 350 Series Access Point, Content Services Switch 11000 Series (WebNS), MGX 8200 Series Edge Concentrators, MGX 8800 Series Multiservice Switches, MGX 8900 Series Multiservice Switches, SN5400 Series Storage Routers; OpenBSD 3.x; Hitachi GR2000 Series Gigabit Routers, GR4000 Series Gigabit Routers, GS3000 Series Gigabit Switches, GS4000 Series Gigabit Switches; ALAXALA Networks AX5400S, AX7800R, AX7800S; FreeBSD FreeBSD 2.x, 3.x, 4.x	A remote Denial of Service vulnerability has been reported in the Protection Against Wrapped Sequence Numbers (PAWS) technique that was included to increase overall TCP performance. Update information available at: http://www.cisco.com/warp/ public/707/cisco-sn-20050518-tcpts.shtml OpenBSD: ftp://ftp.openbsd.org/pub/OpenBSD/ patches/3.6/common/015_tcp.patch Hitachi: The vendor has issued updated versions. ALAXALA: Customers are advised to contact the vendor in regards to obtaining and applying the appropriate update. Microsoft: http://www.microsoft.com/ technet/security/advisory/ 899480.mspx **FreeBSD:** **http://www.freebsd.org/cgi/ cvsweb.cgi/src/sys/netinet/ tcp_input.c** An exploit script has been published.	Cisco Various Products TCP Timestamp Denial of Service CAN-2005-0356	Low	Cisco Security Notice, 64909, May 18, 2005 Microsoft Security Advisory (899480), May 18, 2005 **US-CERT VU#637934** **FreeBSD CVS Log, May 25, 2005**

MyBulletinBoard MyBulletinBoard RC4	A vulnerability has been reported due to insufficient sanitization of input passed to the 'website' field when updating user profiles, which could let a remote malicious user execute arbitrary HTML and script code. Patch available at: http://mybboard.com/community/attachment.php?aid=862 There is no exploit code required.	MyBulletinBoard 'website' Arbitrary Code Execution CAN-2005-1811	High	MyBB RC4 Security Update, May 31, 2005
NewLife Blogger NewLife Blogger 3.0, 3.0.1, 3.1, 3.2, 3.2.3, 3.3	Several SQL injection vulnerabilities were reported due to insufficient sanitization of certain unspecified input, which could let a remote malicious user execute arbitrary SQL code. Upgrades available at: http://prdownloads.sourceforge.net/nlb/nlb-3.3.1.zip?download There is no exploit code required.	NewLife Blogger Multiple Unspecified SQL Injection	High	Security Focus, 13815, May 30, 2005
NikoSoft WebMail 0.10-0.10.4	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of unspecified input, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://www.nikosoft.net/nswm/ There is no exploit code required.	NikoSoft WebMail Unspecified Cross-Site Scripting	High	Secunia Advisory, : SA15518, May 30, 2005
Nokia Nokia 9500	A remote Denial of Service vulnerability has been reported when handling a malformed vCard. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Nokia 9500 vCard Viewer Remote Denial of Service CAN-2005-1801	Low	Security Focus, 13784, May 26, 2005
Nortel Networks Contivity 1000 VPN Switch, 1500 VPN Switch, 1600 Secure IP Services Gateway, Contivity 2000 VPN Switch, 2500 VPN Switch, 2600 Secure IP Services Gateway, Contivity 4000 VPN Switch, 4500 Secure IP Services Gateway, Contivity 4600 Secure IP Services Gateway, VPN Router 1010, 1050, 1100, 1700, 1740, 2700, 5000, 600	A remote Denial of Service vulnerability has been reported when processing an IKE main packet (ISAKMP) header of a certain type. Update information available at: http://www130.nortelnetworks.com/cgi-bin/eserv/cs/main.jsp?level=6&category=29&subcategory=1&DocumentOID=328562 Currently we are not aware of any exploits for this vulnerability.	Nortel Networks Multiple Products Remote Denial of Service CAN-2005-1802	Low	Security Focus, 13792, May 31, 2005
NPDS NPDS 4.8, 5.0	Multiple vulnerabilities have been reported: a Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of some input before returning to the user, which could let a remote malicious user execute arbitrary HTML and script code; a Cross-Site Scripting vulnerability has been reported in 'reply.php' due to insufficient sanitization of the 'image_subject' parameter, which could let a remote malicious user execute arbitrary HTML and script code; and an SQL injection vulnerability has been reported in 'modules.php' due to insufficient sanitization of the 'terme' parameter and in 'links.php' due to insufficient sanitization of the 'query' parameter, which could let a remote malicious user execute arbitrary SQL code. Patches available at: http://www.npds.org/download.php?op=geninfo&did=115 There is no exploit code required; however, Proofs of Concept exploits have been published.	NPDS Multiple Input Validation CAN-2005-1804	High	Security Tracker Alert, 1014073, May 29, 2005
NZEO Zeroboard 4.1 pl2-pl5	A vulnerability has been reported due to an insecure implementation of the PHP 'preg_replace' function, which could let a remote malicious user obtain unauthorized access. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	NZEO Zeroboard 'Preg_replace' Remote Unauthorized Access	Medium	Securiteam, May 31, 2005
peercast.org PeerCast 0.1211	A format string vulnerability has been reported when attempting to handling a malformed HTTP GET request, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. Upgrade available at: http://www.peercast.org/download.php	Peercast.org PeerCast Remote Format String CAN-2005-1806	High	GulfTech Security Research , May 28, 2005

	A Proof of Concept exploit has been published.			
PHP Group PHP 4.0-4.0.7, 4.0.7 RC1-RC3, 4.1 .0-4.1.2, 4.2 .0-4.2.3, 4.3-4.3.8, 5.0 candidate 1-3, 5.0 .0-5.0.2	A vulnerability exists in the 'open_basedir' directory setting due to a failure of the cURL module to properly enforce restrictions, which could let a malicious user obtain sensitive information. Ubuntu: http://security.ubuntu.com/ ubuntu/pool/main/p/php4/ FedoraLegacy: http://download.fedoralegacy.org /redhat/ **Conectiva:** **http://distro.conectiva.com.br/ atualizacoes/index.php?id= a&anuncio=000957** There is no exploit code required; however, a Proof of Concept exploit has been published.	PHP cURL Open_Basedir Restriction Bypass CAN-2004-1392	Medium	Security Tracker Alert ID, 1011984, October 28, 2004 Ubuntu Security Notice, USN-66-1, January 20, 2005 Ubuntu Security Notice, USN-66-2, February 17, 2005 Fedora Legacy Update Advisory, FLSA:2344, March 7, 2005 **Conectiva Security Advisory, CLSA-2005:957, May 31, 2005**
PHP Group PHP prior to 5.0.4; Peachtree Linux release 1	Multiple Denial of Service vulnerabilities have been reported in 'getimagesize().' Upgrade available at: http://ca.php.net/get/php-4.3.11.tar.gz/from/a/mirror Ubuntu: http://security.ubuntu.com/ ubuntu/pool/main/p/php4/ Slackware: ftp://ftp.slackware.com/ pub/slackware/ Debian: http://security.debian.org/ pool/updates/main/p/php3/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Gentoo: http://security.gentoo.org/ glsa/glsa-200504-15.xml Mandrake: http://www.mandrakesecure.net/ en/ftp.php Peachtree: http://peachtree.burdell.org/ updates/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/ TurboLinux/TurboLinux/ia32/ RedHat: http://rhn.redhat.com/ errata/RHSA-2005-405.html SGI: ftp://patches.sgi.com/support/ free/security/advisories/ **Debian:** **http://security.debian.org/ pool/updates/main/p/php4/** Currently we are not aware of any exploits for these vulnerabilities.	PHP 'getimagesize()' Multiple Denials of Service CAN-2005-0524 CAN-2005-0525	Low	iDEFENSE Security Advisory, March 31, 2005 Ubuntu Security Notice, USN-105-1, April 05, 2005 Slackware Security Advisory, SSA:2005-095-01, April 6, 2005 Debian Security Advisory, DSA 708-1, April 15, 2005 SUSE Security Announcement, SUSE-SA:2005:023, April 15, 2005 Gentoo Linux Security Advisory, GLSA 200504-15, April 18, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:072, April 19, 2005 Peachtree Linux Security Notice, PLSN-0001, April 21, 2005 Turbolinux Security Advisory, TLSA-2005-50, April 28, 2005 RedHat Security Advisory, RHSA-2005:405-06, April 28, 2005 SGI Security Advisory, 20050501-01-U, May 5, 2005 **Debian Security Advisory, DSA 729-1, May 26, 2005**
PHPMailer PHPMailer 1.7-1.7.2	A remote Denial of Service vulnerability has been reported in 'class.smtp.php' due to an error when processing overly long headers in the 'Data()' function. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	PHPMailer 'Data()' Function Remote Denial of Service CAN-2005-1807	Low	Security Tracker Alert, 1014069, May 28, 2005

phppc.de PHP Poll Creator 1.01	A vulnerability has been reported in 'poll_vote.php' due to insufficient verification of the 'relativer_pfad' parameter, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	PHP Poll Creator 'relativer_pfad' File Inclusion Vulnerability CAN-2005-1755	High	Secunia SA15510, May 26, 2005
PowerScripts.org PowerDownload 3.0.2, 3.0.3	A vulnerability has been reported in 'pdl-inc/pdl_header.inc.php' due to insufficient validation of the 'incdir' variable, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	PowerDownload 'incdir' Variable Remote Code Execution	High	SoulBlack Security Research, May 31, 2005
Qualiteam Corp. X-Cart 4.0.8	Some input validation vulnerabilities have been reported due to insufficient validation of user-supplied input in several parameters, which could let a remote malicious user execute arbitrary SQL commands or arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	Qualiteam X-Cart SQL Injection & Cross-Site Scripting	High	SVadvisory#7, May 29, 2005
Sony Ericsson P900	A remote Denial of Service vulnerability has been reported in the Bluetooth-related Beamer application when handling a malformed file. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Sony Ericsson P900 Beamer Malformed File Name Handling Remote Denial of Service CAN-2005-1809	Low	Security Focus, 13782, May 26, 2005
WordPress WordPress 1.5, 1.5.1	An SQL injection vulnerability has been reported due to insufficient sanitization of the 'cat_ID' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. Upgrades available at: http://wordpress.org/latest.tar.gz There is no exploit code required.	Wordpress Cat_ID Parameter SQL Injection CAN-2005-1810	High	Secunia Advisory, SA15517, May 30, 2005
ZPanel ZPanel 2.0, 2.5 beta9 & beta 10, 2.5 beta	Multiple vulnerabilities have been reported: a vulnerability has been reported in 'index.php' due to insufficient sanitization of the 'uname' parameter, which could let a remote malicious user execute arbitrary SQL code; and a vulnerability has been reported because installation scripts are not properly removed after installation, which could let a remote malicious user reinstall an affected installation. No workaround or patch available at time of publishing. **An exploit script has been published.**	ZPanel Multiple SQL Injection and File Include CAN-2005-0792 CAN-2005-0793 CAN-2005-0794	High	Secunia Advisory, SA14602, March 16, 2005 **Security Focus, 12809, May 30, 2005**

[back to top]

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
May 31, 2005	Strong2boom.zip	No	Proof of Concept exploit for the Firefly Studios Stronghold 2 Remote Denial of Service vulnerability.
May 31, 2005	zeroboard.c	No	Exploit for the Zeroboard 'Preg_replace' Remote Command Execution vulnerability.
May 30, 2005	elfcd.sh	Yes	Exploit for the Multiple Vendors Linux Kernel ELF Core Dump Buffer Overflow vulnerability.
May 30, 2005	nikto-1.35.tar.gz	N/S	A perl open source web server scanner which supports SSL. Nikto checks for (and if possible attempts to exploit) over 2400 remote web server vulnerabilities and misconfigurations.
May 30, 2005	rkhunter-1.2.7.tar.gz	N/A	Rootkit Hunter scans files and systems for known and unknown rootkits, backdoors, and sniffers.

May 30, 2005	zpanel-sql-exp.pl r57zpanel.pl.txt	No	Exploits for the ZPanel Multiple SQL Injection and File Include vulnerability.
May 28, 2005	npds_sql_poc	Yes	Proof of Concept exploit for the NPDS Multiple Input Validation Vulnerabilities.
May 27, 2005	4DWebStar.c	Yes	Script that exploits the 4D WebStar Tomcat Plugin Remote Buffer Overflow vulnerability.
May 27, 2005	5BP0D00FPI.pl.txt	Yes	Exploit for the Ethereal DistCC buffer overflow vulnerability.
May 27, 2005	arpus CE.pl arpusCE.c	No	Scripts that exploit the Robert Styma Consulting ARPUS/Ce Buffer Overflow & Race Condition vulnerabilities.
May 27, 2005	BulletProof.c	No	Script that exploits the BulletProof FTP Server Privilege Escalation vulnerability.
May 27, 2005	DataTracConsole.c	No	Script that exploits the Randy Wable datatrac Denial of Service Vulnerability.
May 27, 2005	dmail_expl.c	No	Script that exploits the dSMTP mail server 3.1b remote root format string vulnerability.
May 27, 2005	elfcd1.txt	Yes	Exploit for the Multiple Vendors Linux Kernel ELF Core Dump Buffer Overflow vulnerability.
May 27, 2005	ESRI9x.c	Yes	Script that exploits the ESRI ArcInfo Workstations Format String vulnerability.
May 27, 2005	ethereal-SMB-DoS.c	Yes	Denial of Service exploit for the Ethereal SMB vulnerability.
May 27, 2005	exploit_icon.zip	No	Proof of Concept exploit for the Microsoft Windows 'User32.DLL' Icon Handling Denial of Service vulnerability.
May 27, 2005	FilePocket12.c	No	Exploit for the FilePocket Local Information Disclosure vulnerability.
May 27, 2005	firefox0day.php.txt	Yes	Mozilla Firefox 1.0.3 remote arbitrary code execution exploit.
May 27, 2005	firefoxSploit.txt	Yes	Mozilla Firefox view-source:javascript url code execution exploit proof of concept.
May 27, 2005	firefoxSploit-2.txt	Yes	Mozilla Suite and Firefox script objections command execution exploit.
May 27, 2005	fusion_v3.6.1_exploit.txt	No	Exploit for the Fusion versions 3.6.1 and below headline_temp.php injection vulnerability.
May 27, 2005	gaimpoc.c	Yes	Proof of Concept exploit for the GAIM 1.2.x URL handling remote buffer overflow vulnerability.
May 27, 2005	goldenFTP25200.c goldenFTPbof.c	No	Scripts that exploit the Golden FTP Server Pro version 2.52.0.0 remote stack buffer overflow vulnerability.
May 27, 2005	GoText101.c	No	Script that exploits the StumbleInside GoText Discloses Users Configuration Data vulnerability.
May 27, 2005	hosting061.txt	No	Hosting Controller versions 0.6.1 and below unauthenticated user registration exploit.
May 27, 2005	hosting061-2.c	No	Hosting Controller versions 0.6.1 and below unauthenticated user registration exploit.
May 27, 2005	hpuxFTPd112144.c	Yes	HP-UX ftpd versions 1.1.214.4 and below REST remote brute force exploit.
May 27, 2005	HS_WINS.cpp	N/A	Microsoft WINS remote operating system and service pack scanner.
May 27, 2005	ICUII70.c	No	Script that exploits the Cybration ICUII Password Disclosure vulnerability.
May 27, 2005	IMail.pl	Yes	Perl script that exploits the IMail Commerce i-mail.cgi remote command execution vulnerability.
May 27, 2005	invision203Login.pl.txt	Yes	Exploit for the Invision Power Cross-Site Scripting & SQL Injection vulnerability.
May 27, 2005	LandIpV6.c	Yes	Microsoft Windows XP/2003 IPv6 remote denial of service vulnerability.
May 27, 2005	maxdb_webdbm_get_overflow.pm MaxDB750023.c	Yes	Scripts that exploits the MySQL MaxDB Remote Buffer Overflows vulnerabilities.
May 27, 2005	maxwebportal136-1.txt maxwebportal136-2.txt maxwebportal136-3.txt	No	Exploits for the Maxwebportal versions 1.36 and below password.asp Change Password vulnerability.
May 27, 2005	msmq_deleteobject_ms05_017.pm	Yes	This Metasploit module exploits a stack overflow in the RPC interface to the Microsoft.
May 27, 2005	netvault.c	No	Script that exploits the BakBone NetVault Remote Heap Overflow Code Execution vulnerability.
May 27, 2005	NotJustBrowsing.c	No	Script that exploits the NetLeaf Limited NotJustBrowsing Discloses Application Password vulnerability.
May 27, 2005	pktcdvd_dos.c	Yes	Denial of Service exploit for the Linux kernel ioctl_by_bdev() vulnerability.
May 27, 2005	postnukeInclusion.txt	Yes	Exploit for the Postnuke versions 0.750 through 0.760rc4 file inclusion vulnerability.
May 27, 2005	r57ipb2.pl.txt	Yes	Exploit for the Invision Power Cross-Site Scripting & SQL Injection vulnerability.
May 27, 2005	RatBof.cpp	Yes	Internet Explorer content advisor exploit that is related to MS05-020.
May 27, 2005	Snmppd.c	No	Script that exploits the SNMPPD SNMP Proxy Daemon Remote Format String vulnerability.
May 27, 2005	tcptimestamps.c	Yes	Script that exploits the Multiple Vendor TCP Timestamp Denial of Service vulnerability.
May 27, 2005	wwwguestbook.txt	No	Exploit for the WWWguestbook SQL Injection vulnerability.
May 27, 2005	ZeroBoardWorm.c	N/A	Worm source code that exploits a vulnerability in ZeroBoard, allowing arbitrary PHP code injection.
May 26, 2005	cnedrabof.zip	No	Exploit for the C'Nedra Network Plug-in 'Read_TCP_String' Remote Buffer Overflow vulnerability.

May 26, 2005	invision_sql_poc.pl	Yes	Script that exploits the Invision Power Cross-Site Scripting & SQL Injection vulnerability.
May 26, 2005	sbphpstatpoc.txt	No	Proof of Concept exploit for the PHPStat Setup.PHP Authentication Bypass Vulnerability.
May 26, 2005	t3wmbof.zip	No	Exploit for the Clever's Games Terminator 3: War of the Machines Server Buffer Overflow vulnerability.
May 25, 2005	cryptoloop_exploit.tar cryptoloop-exploit.tar.bz2	No	Scripts that exploit the Linux Kernel Cryptoloop Information Disclosure vulnerability.

[back to top]

Trends

- **EU zombie army leads the world:** The European Union leads the world in the number of computers that are controlled remotely by hackers. Data from email security specialist CipherTrust shows that 26 per cent of all PCs infected in May are located in the EU, compared with 20 per cent in the US and 15 per cent in China. The UK accounted for three per cent of the world's total, with Germany leading Europe at six per cent. Over May an average of 172,000 new PCs were infected each month. Source: http://www.vnunet.com/vnunet/news/2135706/eu-zombie-army-leads-world.
- **Bank of America to use two-factor system to beat phishers:** In an attempt to reduce identity theft and reduce the threat of phishing attacks, the Bank of America plans to introduce two-factor, two-way authentication to around 13 million online banking customers. Unlike traditional two-factor authentication, the Bank of America's Sitekey approach uses a customer's PC or handheld device as the second-factor hardware device. Technology from security company Passmark takes a "fingerprint" of a customer's computer to verify identification, using HHTP headers, software configurations, hardware settings, IP address and geographic location. Source: http://www.computerweekly.com/Article138764.htm?src=rssNews.
- **Identity theft fears most US Citizens:** Despite a recent push in identity theft prevention awareness by major organizations and government agencies, 75 percent of US citizens believe that their identity is no more secure than one year ago. Consumers do not believe current and traditional methods of security are good enough to protect them against identity theft. Source: http://www.it-observer.com/articles.php?id=735.

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), approximate date first found, and brief description.

Rank	Common Name	Type of Code	Trend	Date	Description
1	Netsky-P	Win32 Worm	Stable	March 2004	A mass-mailing worm that uses its own SMTP engine to send itself to the email addresses it finds when scanning the hard drives and mapped drives. The worm also tries to spread through various file-sharing programs by copying itself into various shared folders.
2	Netsky-Q	Win32 Worm	Stable	March 2004	A mass-mailing worm that attempts to launch Denial of Service attacks against several web pages, deletes the entries belonging to several worms, and emits a sound through the internal speaker.
3	Mytob.C	Win32 Worm	Stable	March 2004	A mass-mailing worm with IRC backdoor functionality which can also infect computers vulnerable to the Windows LSASS (MS04-011) exploit. The worm will attempt to harvest email addresses from the local hard disk by scanning files.
4	Zafi-D	Win32 Worm	Stable	December 2004	A mass-mailing worm that sends itself to email addresses gathered from the infected computer. The worm may also attempt to lower security settings, terminate processes, and open a back door on the compromised computer.
5	Netsky-D	Win32 Worm	Stable	March 2004	A simplified variant of the Netsky mass-mailing worm in that it does not contain many of the text strings that were present in NetSky.C and it does not copy itself to shared folders. Netsky.D spreads itself in e-mails as an executable attachment only.
6	Lovgate.w	Win32 Worm	Stable	April 2004	A mass-mailing worm that propagates via by using MAPI as a reply to messages, by using an internal SMTP, by dropping copies of itself on network shares, and through peer-to-peer networks. Attempts to access all machines in the local area network, terminate certain processes and create archived files on the infected machine. Has backdoor capabilities, which enables it to open random ports on and steal information.

7	Zafi-B	Win32 Worm	Stable	June 2004	A mass-mailing worm that spreads via e-mail using several different languages, including English, Hungarian and Russian. When executed, the worm makes two copies of itself in the %System% directory with randomly generated file names.Zafi.B prevents the user from using applications that contain the strings "regedit" "msconfig" and "task" in the filename.
7	Netsky-Z	Win32 Worm	Stable	April 2004	A mass-mailing worm that is very close to previous variants. The worm spreads in e-mails, but does not spread to local network and P2P and does not uninstall Bagle worm. The worm has a backdoor that listens on port 665.
9	Netsky-B	Win32 Worm	Stable	February 2004	A mass-mailing worm that uses its own SMTP engine to send itself to the email addresses it finds when scanning the hard drives and mapped drives. Also searches drives for certain folder names and then copies itself to those folders.
10	MyDoom-O	Win32 Worm	Stable	July 2004	A mass-mailing worm that uses its own SMTP engine to generate email messages. It gathers its target email addresses from files with certain extension names. It also avoids sending email messages to email addresses that contain certain strings.

[back to top]

Last updated June 01, 2005